IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:	
Daniel M. WONG et al.	Group Art Unit: 2139
Serial No.: 10/600,388	Examiner: Jackson, Jenise E.
Filed: June 20, 2003	Confirmation No. 8538
For: METHOD AND APPARATUS FOR ENABLING DATABASE PRIVILEGES	

REQUEST FOR CONTINUED EXAMINATION UNDER 37 C.F.R. 1.114 WITH AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the final Office Action mailed March 14, 2008, Applicants request for continued examination under 37 C.F.R. § 1.114 and amend the above-identified application as follows.

Amendments to the Claims begin on page 2.

Remarks begin on page 7.

AMENDMENTS TO THE CLAIMS

Please amend claims 1, 14 and 26 as set forth below, without acquiescence in the Office Action's reasons for rejection or prejudice to pursue in a related application. A complete listing of the pending claims is provided below.

1. (Currently Amended) A method for enabling privileges comprising:

establishing a session on behalf of a user;

receiving a request to enable database privileges for the user;

upon receipt of the request to enable database privileges, verifying trusted security logic has previously been executed, wherein the act of verifying the trusted security logic comprises verifying a proxy user and checking a call stack; and

enabling database privileges for the user if the trusted security logic has previously been executed and is contained in one or more frames of the call stack.

2. (Previously Presented) The method of claim 1, further comprising:

storing call information in one or more frames of the call stack; and wherein

the act of verifying further comprises determining whether the one or more frames of the call stack corresponds to the trusted security logic.

3. (Previously presented) The method of claim 1, wherein the act of verifying the trusted security logic further comprises verifying an application name.

4. (Original) The method of claim 3, wherein the act of verifying the trusted security logic further includes verifying a security function name.

5. (Previously presented) The method of claim 1, wherein the act of verifying trusted security logic further comprises verifying a module name.

6. (Original) The method of claim 1, further comprising:

collecting one or more session parameters;

comparing the one or more session parameters against a set of trusted security parameters defined in a security function; and

returning a result indicating whether the one or more session parameters matches the set of trusted security parameters.

7. (Cancelled)

8. (Original) The method of claim 1, further comprising:

receiving information identifying the user;

prompting the user for a password;

authenticating the user based on information stored in an application program; and

associating the user with a role.

9. (Previously presented) A client-server computer system comprising:

a computer including:

a processor,

a main memory communicatively coupled to the processor; and

a disk storage communicatively coupled to the processor;

a database running on the computer from the main memory, the database further comprising:

one or more data structures stored in the disk storage, and

a call stack stored in the main memory;

an application program coupled to the database and configured to support a user; and

a metadata repository embodied in the one or more data structures stored in the disk storage, the metadata repository comprising trusted security logic; wherein

the application program is configured to initiate a call to enable database privileges, the call causing information to be stored in one or more frames of the call stack and one or more security functions to be executed; and wherein

the database is configured to:

verify the call stack comprises one or more frames corresponding to the trusted security logic;

test a proxy user; and

enable database privileges for the user if the trusted security logic is contained in the one or more frames of the call stack.

10. (Original) The client-server computer system of claim 9, wherein the application program resides with the database in the computer.

11. (Original) The client-server computer system of claim 9, wherein the application program resides on a separate computer communicatively coupled to the database.

12. (Original) The client-server computer system of claim 9, wherein the trusted security logic includes a schema name and a security package name.

13. (Cancelled)

14. (Currently Amended) A computer-readable medium having stored therein one or more sequences of instruction for enabling privileges, the one or more sequences of instructions causing one or more processors to perform a number of acts, said acts comprising:

establishing a session on behalf of a user;

receiving a request to enable database privileges for the user;

upon receipt of the request to enable database privileges, verifying trusted security logic has previously been executed, wherein the act of verifying the trusted security logic comprises verifying a proxy user and checking a call stack; and

enabling database privileges for the user if the trusted security logic has previously been executed and is contained in one or more frames of the call stack.

15. (Previously Presented) The computer-readable medium of claim 14, further comprising:

storing call information in one or more frames of the call stack; and wherein

the act of verifying further comprises determining whether the one or more frames of the call stack corresponds to the trusted security logic.

16. (Previously presented) The computer-readable medium of claim 14, wherein the act of verifying the trusted security logic further comprises verifying an application name.

17. (Original) The computer-readable medium of claim 16, wherein the act of verifying the trusted security logic further includes verifying a security function name.

18. (Previously presented) The computer-readable medium of claim 14, wherein the act of verifying trusted security logic further comprises verifying a module name.

19. (Original) The computer-readable medium of claim 14, further comprising:

collecting one or more session parameters;

comparing the one or more session parameters against a set of trusted security parameters defined in a security function; and

returning a result indicating whether the one or more session parameters matches the set of trusted security parameters.

20. (Cancelled)

21. (Original) The computer-readable medium of claim 14, further comprising:
receiving information identifying the user;
prompting the user for a password;
authenticating the user based on information stored in an application program; and
associating the user with a role.

22-25. (Cancelled)

26. (Currently Amended) A system for enabling privileges comprising:
means for establishing a session on behalf of a user;
means for receiving a request to enable database privileges for the user;
means for upon receipt of the request to enable database privileges, verifying trusted security logic has previously been executed, wherein means for verifying the trusted security logic comprises means for verifying a proxy user and checking a call stack; and
means for enabling database privileges for the user if the trusted security logic has previously been executed and is contained in one or more frames of the call stack.

27. (Previously Presented) The system of claim 26, further comprising:
means for storing call information in one or more frames of the call stack; and
wherein
means for verifying further comprises means for determining whether the one or more frames of the call stack corresponds to the trusted security logic.

28. (Previously presented) The system of claim 26, wherein means for verifying the trusted security logic further comprises means for verifying an application name.

29. (Previously presented) The system of claim 28, wherein means for verifying the trusted security logic further comprises means for verifying a security function name.

30. (Previously presented) The system of claim 22, wherein means for verifying trusted security logic further comprises means for verifying a module name.

31. (Previously presented) The system of claim 22, further comprising:

means for collecting one or more session parameters;

means for comparing the one or more session parameters against a set of trusted security parameters defined in a security function; and

means for returning a result indicating whether the one or more session parameters matches the set of trusted security parameters.

32. (Previously presented) The system of claim 22, further comprising:

means for receiving information identifying the user;

means for prompting the user for a password;

means for authenticating the user based on information stored in an application program; and

means for associating the user with a role.

REMARKS

Claims 1-6, 8-12, 14-19, 21 and 26-32 are currently pending in the application. In the Office Action dated March 14, 2008, claims 1-6, 8, 14-19, 21 and 26-32 have been rejected, and claims 9-12 have been allowed. By this Amendment, claims 1, 14 and 26 have been amended, without acquiescence or prejudice to pursue the original claims in a related application. No new matter has been added.

Allowable Subject Matter

Applicants thank the Examiner for indicating that claims 9-12 are allowed.

Claim Rejections - 35 USC § 103

Claims 1-6, 14-19, and 26-31, are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernstein et al. (5,884,316) in view of Mallory (6,126,328).

These rejections are improper because Mallory cannot be used to preclude patentability under 35 U.S.C. 103(c). Mallory is a 102(e) reference, and the present application and Mallory have common assignee at the time of the invention of the present application.

102(e) Reference

The present application has a priority filing date of June 29, 1999. The Mallory reference was filed on February 28, 1997 and was patented on October 3, 2000. Therefore, Mallory is a 102(e) reference with respect to the present application. In addition, Mallory does not qualify as a 102(a), (b), (c) or (d) reference.

Common Ownership

The present application and Mallory were, at the time the invention of the present application was made, owned by Oracle International Corporation. (see MPEP 7706.02(l)(2)).

Therefore, Mallory cannot be used to preclude patentability under 35 U.S.C. 103(c). (see MPEP 706.02(l)(3)). For at least the above reasons, Applicants requests that the 35 U.S.C. 103(a) rejections for claims 1-9 and 17-20 be withdrawn.

In addition, claim 1, as amended, recites the limitation "enabling database privileges for the user if the trusted security logic has previously been executed and is contained in one or more frames of the call stack" (emphasis added). Claims 14 and 26 have similar limitations.

As stated in the Office Action, the limitation "enable database privileges for the user if the trusted security logic is contained in the one or more frames of the call stack" is not disclosed in the cited references. Amended claims 1, 14 and 26 all recite these limitations.

For at least these reasons, Applicants submit that Bernstein in view of Mallory fails to disclose, teach or suggest every limitation of claim 1. Because claims 14 and 26 have similar limitations to claim 1 as discussed above, claims 14 and 26 are allowable. Furthermore, because claims 2-6, 15-19, and 27-31 depend from claims 1, 14, and 26, they also are allowable for at least the same reasons.

Claims 8, 21, and 32, are rejected under 35 U.S.C. 103(a) as being unpatentable over Bernstein (5, 884,316) in view of Mallory further in view of Fisher et al. (6,092,189).

As discussed above, Mallory cannot be used to preclude patentability under 35 U.S.C. 103(c). (see MPEP 706.02(l)(3)). Moreover, the Office Action states that the limitation "enable database privileges for the user if the trusted security logic is contained in the one or more frames of the call stack" is not disclosed or suggested by any of the cited references. Thus, these claims are also allowable.

CONCLUSION

Based on the foregoing, all claims are believed allowable, and an allowance of the claims is respectfully requested. If the Examiner has any questions or comments, the Examiner is respectfully requested to contact the undersigned at the number listed below.

To the extent that any arguments and disclaimers were presented to distinguish prior art, or for other reasons substantially related to patentability, during the prosecution of any and all parent and related application(s)/patent(s), Applicant(s) hereby explicitly retracts and rescinds any and all such arguments and disclaimers, and respectfully requests that the Examiner re-visit the prior art that such arguments and disclaimers were made to avoid.

Credit card payment by USPTO - EFS in the amount of $810.00 is charged herein.

The Commissioner is authorized to charge Vista IP Law Group LLP Account No. 50-1105 for any fees required that are not covered, in whole or in part, and to credit any overpayments to said Deposit Account No. 50-1105.

Respectfully submitted,

Dated: June 16, 2008

By: 
Jasper Kwoh
Registration No. 54,921

Vista IP Law Group LLP
1885 Lundy Avenue,
Suite 108
San Jose, CA 95131
Telephone: (408) 321-8663